



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,447	10/09/2001	Edward R. Rowe	07844-448001	7875
21876	7590	06/20/2006	EXAMINER	
FISH & RICHARDSON P.C. P.O. Box 1022 MINNEAPOLIS, MN 55440-1022			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/973,447		ROWE, EDWARD R.	
	Examiner		Art Unit	
	Jung Kim		2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-36 and 38 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-17,23-29 and 32-36 is/are rejected.
- 7) ☒ Claim(s) 18-22,30,31 and 38 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. This Office action is in response to the amendment filed on 5/11/06.
2. Claims 1, 2, 4-36 and 38 are pending.
3. Claims 3 and 37 are canceled.

Response to Amendment

4. The 112/2nd paragraph rejection to claim 37 is withdrawn as the claim is canceled.
5. The 112/2nd paragraph rejection to claim 25 is withdrawn as the amendment overcomes the 112/2nd paragraph rejection.

Response to Arguments

6. On pgs. 11-12, applicant argues that Peinado does not disclose the limitation of a second key encrypting a first key, wherein the first key encrypts a document decryption key. In particular, applicant argues:

The examiner stated that Peinado discloses an encrypted document key, an encrypted first key, and a second key. The applicant disagrees. Even if one assumes for argument's sake that KD corresponds to the encrypted document key and PR-BB corresponds to the first key, Peinado does not disclose the second key.

The examiner looks to column 23, lines 6-24 of Peinado for the limitation of having a second key. There Peinado discloses a way of hiding a private key from the world. (A "private key" is part of a private-key and public-key pair for use in public-key cryptography.) Peinado teaches that one way to hide this private key is to split it into several sub-components, encrypting each sub-component

separately, then storing each separately in a different location. That is to say, Peinado teaches splitting one private key into several pieces. No piece is useful on its own, because each is only a piece of a key and not a whole key. By teaching only a single private key, Peinado does not teach two separate keys (a first key and a second key). In particular Peinado does not teach a second key which encrypts a first key, where the first key encrypts a document decryption key. Additionally, even if assuming for argument's sake that the PR-BB key corresponds to the recited first key, Peinado does not teach that the PR-BB key is encrypted. (pg. 11, last paragraph-pg. 12, 2nd paragraph)

7. It is first noted that the limitations of claim 1 do not suggest the limitation of "a second key which encrypts a first key, where the first key **encrypts** a document decryption key" as recited in the quoted portion of applicant's arguments above. In fact, the claims recite a second key encrypting a first key, wherein the first key **decrypts** an encrypted document decryption key. It is assumed here that this is a typographical error and in fact applicant's argument is suggesting that the prior art does not teach a second key encrypting a first key, wherein the first key **decrypts** an encrypted document decryption key.

8. In reply to applicant's argument that Peinado does not disclose the aforementioned limitation, examiner disagrees. Peinado expressly discloses a private key (PR-BB) used to decrypt an encrypted document decryption key (KD) (see figure 5B, reference nos. 523 and 529), wherein the private key (PR-BB) is encrypted using another key (col. 23:16-20; "In one embodiment of the present invention, such private key (PR-BB) is encrypted according to code-based encryption techniques. In particular, in such embodiment, the actual software code of the black box 30 (or other software

Art Unit: 2132

code) is employed as encrypting key(s).") As shown here, applicant's allegation that "Peinado does not teach the PR-BB is encrypted" is patently false. This disclosure of Peinado clearly indicates a second key encrypting a first key and the first key decrypting an encrypted document. Hence, the rejection of claim 1 is maintained.

9. Applicant's arguments with respect to amended claim 10 have been considered but are moot in view of the new ground(s) of rejection.

10. On pgs. 13-14, applicant argues that Peinado does not suggest or teach the limitation of claim 13. In particular, Applicant allege:

Peinado teaches that there is precisely one way to decrypt digital content: by using the black box's private key to decrypt the license's encrypted decryption key, and then using that decryption key to decrypt the digital content. Even assuming for argument's sake that Peinado's decryption key corresponds to the applicant's document encryption key and Peinado's black box private key corresponds to the applicant's first key, Peinado does not teach any way of providing the document decryption key without using the first key. By contrast, claim 13 recites "providing a document encryption key in an access-controlled manner to users for accessing the document without using the first key." (pg. 14, 3rd full paragraph)

11. Contrary to applicant's suggestion, it is noted that amended claim 13 recites "providing a document decryption key in an access controlled manner to users for opening the encrypted document without using the first key." In reference to the rejection of this limitation of claim 13, Peinado clearly discloses "providing a document decryption key in an access controlled manner to users for opening the encrypted

document without using the first key," since only the document decryption key is required to decrypt the encrypted document; the first key is only required when decrypting the document decryption key when the document decryption key is encrypted. If applicant has a different limitation in mind, the claim must be amended to define this different limitation without any ambiguity to the claimed feature. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Hence, the rejection of claim 13 is maintained.

12. In reply to applicant's argument that the combination of Peinado and Richards does not disclose the limitations of claim 32, examiner disagrees. Richards discloses providing encryption keys SK, SK_A0, SK_B0, SK_C0, PK and CUSTOMER_CODE in a secure manner to decrypt multiple programs (col. 6:45-60; 8:60-63; 10:33-49) which anticipates the limitation providing in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents; Richards further discloses using a single key to encrypt all the programs (col. 6:10-7:21) which anticipates the limitation where a single skeleton key can be used to open multiple encrypted documents; Richard further discloses using multiple keys to encrypt a document (col. 8:44-64) which anticipates the limitation a single encrypted document can be opened using more than one skeleton key; and Richard further discloses using a key (CUSTOMER_CODE) to encrypt SK (col. 6:63) or a key (PK) to encrypt SK (col. 9:14-18) which anticipates the limitation a single skeleton key can be opened using one or more other skeleton keys.

Finally, the remaining limitations as well as the motivation to combine Peinado and Richards are consistent with the limitations and motivation to combine as outlined in the rejections of claims 4-7 below. Hence, the rejection of claim 32 is maintained.

13. Applicant's argument that the combined teachings of Peinado and Stallings do not teach the limitations of claim 26 appear to be based on the premise that Stallings does not disclose a collection of at least three keys as recited. However, Stallings clearly discloses the use of a key ring to store and organize in a systematic way for efficient and effective use of a plurality of public/private key pairings. (pg. 365, "Key Rings") Hence, applicant's argument is not persuasive. The rejection of claim 26 is maintained.

14. Applicant's arguments with respect to the prior art rejections of claims 2, 4-9, 11, 12, 14-17, 23, 24, 27-29 and 33-36 are consistent with the arguments outlined above, and therefore these arguments are not persuasive. The rejections of these claims are maintained as well.

Claim Rejections - 35 USC § 102

15. Claims 1, 11, 13-16, 23 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Peinado et al. USPN 6,772,340 (hereinafter Peinado).

16. As per claim 1, Peinado discloses a computer-implemented method for managing access to electronic documents, comprising:

- a. associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key; (fig. 5a, reference nos. 513, 515 and 517; fig. 5b, reference nos. 519, 521 and 523; col. 16:6-14; 17:12-30; 17:49-18:8; 23:58-24:10).
- b. encrypting the first key to produce an encrypted first key; associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the first key (col. 23:6-24; fig. 5a, reference no 517 and fig. 5b, reference nos. 519, 521 and 523).

17. As per claim 11, Peinado discloses the method further comprising storing the encrypted first key in rights management file information for the first key (col. 24:53-67).

18. As per claim 13, Peinado discloses the method further comprising providing a document decryption key in an access controlled manner to users for opening the encrypted document without using the first key (col. 15:53-16:4).

19. As per claim 14, Peinado discloses the method further comprising associating a unique identifier with the first key (fig. 3 and 8; content id and key id).

20. As per claim 15, Peinado further discloses the unique identifier is stored in the document in association with the encrypted document decryption key to associate the first key with the encrypted document decryption key (fig. 3).

21. As per claim 16, Peinado further discloses the rights management information provides a license and defines a set of permission rights associated with the license (col. 24:53-67).

22. As per claim 23, Peinado discloses the encrypted document decryption key is encrypted by an encryption key that is different from the first key (col. 16:6-14).

23. As per claim 34, it is a claim corresponding to claim 1 and it does not teach or define above the information claimed in claim 1. Therefore, claim 34 is rejected as being anticipated by Peinado for the same reasons set forth in the rejection of claim 1.

Claim Rejections - 35 USC § 103

24. Claim 2 is rejected under 35 USC 103(a) as being unpatentable over Peinado in view of Takeda '189 USPN 6,336,189 (hereinafter Takeda '189).

25. As per claim 2, the rejection of claim 1 under 35 USC 102(e) is incorporated herein. (supra) Peinado does not disclose storing the encrypted document key in the encrypted document. Takeda '189 discloses encrypting a decryption key, the decryption key being used to decrypt a program, wherein the encrypted decryption key is appended to a partially encrypted program (col. 8:36-50). This enables instant access to the decryption key to unwrap the program. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to store the encrypted document key in the encrypted document. One would be motivated to do so to facilitate access to the decryption key and to form a clear association between the key and the encrypted document (Takeda '189, *ibid*). The aforementioned cover the limitations of claim 2.

26. Claims 4-7, 17, 32, 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado in view of Richards USPN 6,069,957 (hereinafter Richards '957).

27. As per claims 4-7, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not disclose a first key that decrypts multiple encrypted document decryption keys, or multiple document decryption keys that decrypts an encrypted document. Richards '957 discloses restricting access to programs whereby program material is encrypted using a key hierarchy, or "key-upon-key" encryption,

whereby one key unlocks another and the last key unlocked decrypts the encrypted program (col. 1:25-30). In this scheme, more than one data decryption key is used for a given program, a different data decryption key is used for each distinct program and the data decryption keys are updated (8:36-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the "key-upon-key" encryption technique with the Digital Rights Management invention of Peinado since it decouples the step of securing the data-decrypting key and the user's private key, and facilitates restricted access by maintaining secure and updated key values (Richards '957, 10:5-12). Hence, the method further comprises:

- c. providing a second encrypted document decryption key for a second encrypted document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the first key is usable to decrypt the second encrypted document decryption key, and associating the first key with the second encrypted document decryption key (Richards '957, 8:36-48; 9:12-10:63; 'SK' is encrypted by either 'PK' or customer_code);
- d. providing a third encrypted document decryption key for the second encrypted document, the third encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the third encrypted document decryption key being encrypted so that a third key is usable to decrypt the third encrypted document decryption key,

associating the third key with the third encrypted document decryption key, and providing the third key in an access controlled manner to users for use in opening the second document (Richards '957, 8:44);

e. associating a third key with a second encrypted document decryption key for a second document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the third key is usable to decrypt the second encrypted document decryption key; encrypting the third key, associating the second key with the encrypted third key, the second key being usable to decrypt the encrypted third key, and providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the third key (Richards '957, 8:44; 9:12-10:63).

28. The aforementioned cover the limitations of claims 4-7.

29. As per claim 17, the rejection of claim 16 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not expressly disclose the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key. Richards '957 discloses restricting access to programs whereby program material is encrypted using a key hierarchy, or "key-upon-key" encryption, whereby one key unlocks another and the last key unlocked decrypts the encrypted program (col. 1:25-30). In this scheme, more

Art Unit: 2132

than one data decryption key is used for a given program, a different data decryption key is used for each distinct program and the data decryption keys are updated (8:36-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the "key-upon-key" encryption technique with the Digital Rights Management invention of Peinado since it decouples the step of securing the data-decrypting key and the user's private key, and facilitates restricted access by maintaining secure and updated key values (Richards '957, 10:5-12). The aforementioned cover the limitations of claim 17.

30. As per claims 32, 33 and 36, the rejections of claims 4-7 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys (Richards '957, col. 7:24-33; 8:44-64; 9:12-18). The aforementioned cover the limitations of claims 32, 33 and 36.

31. Claims 8-10, 12, 24-29 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado, and further in view of Stallings, Cryptography and Network Security, Section 6.1 "Principles of Public-Key Cryptosystems," Section 11 "Authentication Applications" and Section 12.1 "Pretty Good Privacy" (hereinafter Stallings).

32. As per claims 8-10, the rejection of claim 1 under 33 USC 102(e) as being anticipated by Peinado is incorporated herein. (supra) Peinado does not disclose the step of providing the second key in an access controlled manner comprises sending the second key to users in rights management information specific to systems of the users to whom the second key is sent and sending information used to synthesize the second key in rights management information; wherein the rights management information comprises a rights management file. Stallings discloses the use of public key certificates to verify the authenticity of a key and enforce the use of the key in limited situations, wherein the certificates include a subject identifier, period of validity, subject's public-key information, a signature to verify the certificate and key, and extension (pg. 342, figure 11.3); the extensions includes key and policy information, which includes key usage, private-key usage period, certificate policies, policy mappings; the key usage attribute in particular indicates the restrictions imposed as to the purposes for which and the policies under which the certified public key may be used. (pgs. 348-349) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the step of providing the second key in an access controlled manner comprises sending the second key to users in rights management information specific to systems of the users to whom the second key is sent and sending information used to synthesize the second key in rights management information; wherein the rights management information comprises a rights management file. One would be motivated to do so to ensure the validity of the key in the rights management information and to indicate security policy information for a given

Art Unit: 2132

key. (pg. 342, "Signature"; pg. 348, requirement 3) The aforementioned cover the limitations of claims 8-10.

33. As per claim 12, the rejection of claim 11 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not expressly disclose associating a unique identifier with the second key and storing the unique identifier in the rights management information with the encrypted first key. Stallings discloses an overview of PGP security, which includes a key management scheme, wherein a key ID is assigned to a key-decrypting key for the purpose of efficiently identifying a key that decrypts an encrypted data decryption key (pg. 365, figure 12.3 and related text). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize key identifiers for the purpose of associating key-decrypting keys to an encrypted data-decrypting key, since it is desirable to efficiently associate such decryption keys with their encrypted values (Stallings, pg. 364, 1st paragraph). The aforementioned cover the limitations of claim 12.

34. As per claim 24, the rejection of claim 23 under 35 USC 102(e) is incorporated herein. (supra) Peinado does not disclose that the encryption key is a private key or that the first key is a public key. However, it is well known in public key encryption that the encryption key of a data value-in this case the document decryption key-can be either the public key or private key. For example, Stallings discloses that in RSA, either of the two keys can be used as the encryption key with the other being used as the

Art Unit: 2132

decryption key (pg. 165, 2nd bullet). The primary deciding factor to determine which is used for encryption is contingent on the desire to ensure the origin of an encrypted document or to ensure the receiver of the encrypted document. In the case of Peinado, private key encryption of the document decryption key would ensure that the encrypted digital content comes from a specific trusted source. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention Peinado so that the encryption key is a private key and the first key is a public key. One would be motivated to so to ensure the origin of the encrypted decryption key and thus ensure the origin of the encrypted document as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 24.

35. As per claim 25, the rejection of claim 24 under 35 USC 103(a) is incorporated herein. (supra) In addition, providing the first key in an access-controlled manner comprises sending information used to synthesize the first key in a rights management file. (Peinado, col. 21:11-62)

36. As per claim 26, Peinado discloses a computer-implemented method for accessing an electronic document comprising:

- f. obtaining an encrypted electronic document (col. 24:41-26:8; especially 25:3-9);
- g. obtaining a collection of three or more keys, the keys including keys that are encrypted, the keys having associations between certain pairs of them,

where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection (col. 23:6-24);

37. Peinado does not expressly disclose explicitly defining the associations.

Stallings discloses an overview of PGP wherein one of the salient features of the invention defines an association between an encrypted data decryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys are sufficient to decrypt the encrypted document (pg. 365, figure 12.3). Moreover, Stallings discloses the use of a key ring to store and organize the keys in a systematic way. (pg. 365, "Key Rings") Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to define the key pair associations and the key/document associations and use the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access for a more efficient means of identifying which keys decrypt which document (Stallings, pg. 363, last paragraph-pg. 364, first paragraph). The aforementioned cover the limitations of claim 26.

Art Unit: 2132

38. As per claims 27 and 28, the rejection of claim 26 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the association of the key-decrypting key decrypting the encrypted data-decrypting key, which decrypts encrypted data defines a directed path, wherein decryption of the encrypted data requires the traversal of a path from a key-decrypting key to the encrypted data. Hence, claims 27 and 28 are covered by the teachings of Peinado and Stallings.

39. As per claim 29, the rejection of claims 27 and 28 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, each encrypted key is identified by two IDs, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key (Stallings, pg. 365, fig. 12.3: key ID of KUb identifies the key capable of decrypting the encrypted data-decrypting key, and the signature uniquely identifies the encrypted key and the encrypted message).

40. As per claim 35, it is a claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 35 is rejected as being unpatentable over Peinado in view of Stallings for the same reasons set forth in the rejection of claim 26.

Allowable Subject Matter

41. Claims 18-22, 30, 31 and 38 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

42. The indicated allowability of claim 25 is withdrawn in view of the amendment to claim 25.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

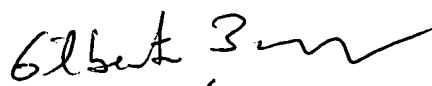
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



June 17, 2006

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100